



Designing a Computational Proof of Cantor's Theorem

Author(s): Edsger W. Dijkstra and Jayadev Misra

Source: *The American Mathematical Monthly*, Vol. 108, No. 5 (May, 2001), pp. 440-443

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2695799>

Accessed: 25/03/2009 14:38

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact support@jstor.org.



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

3. C. Groetsch, The commandant's corollary, *Amer. Math. Monthly* 107 (2000) 15–23.
4. C. Groetsch and B. Cipra, Halley's comment—projectiles with linear resistance, *Math. Mag.* 70 (1997) 273–280.
5. L.N. Long and H. Weiss, The velocity dependence of aerodynamic drag: A primer for mathematicians, *Amer. Math. Monthly* 106 (1999) 127–135.
6. J. Stewart, *Calculus: Concepts and Contexts*, Brooks-Cole, Pacific Grove, CA 1997.

University of British Columbia, Vancouver, B.C. V6T 1Z2, Canada
brauer@math.ubc.ca

Designing a Computational Proof of Cantor's Theorem

Edsger W. Dijkstra and Jayadev Misra

Cantor's Diagonalization The one purpose of this little Note is to show that formal arguments need not be lengthy at all; on the contrary, they are often the most compact rendering of the argument. Its other purpose is to show the strong heuristic guidance that is available to us when we design such calculational proofs in sufficiently small, explicit steps. We illustrate our approach on Georg Cantor's classic diagonalization argument [chosen because, at the time, it created a sensation].

Cantor's purpose was to show that any set S is *strictly* smaller than its powerset $\wp S$ (i.e., the set of all subsets of S). Because of the 1-1 correspondence between the elements of S and its singleton subsets, which are elements of $\wp S$, S is not larger than $\wp S$, and our proof can now be focussed on the “strictly”, i.e., we have to show that there is no 1-1 correspondence between S and $\wp S$. We can confine ourselves to non-empty S .

1. PROOF FORMAT AND NOTATION. Eventually we present our proof in a format, due to W.H.J. Feijen, in which consecutive proof stages are separated by a connective and a justification. Thus,

$$\begin{array}{lcl} & p & \\ \Rightarrow & \{J\} & \\ & q & \\ \equiv & \{M\} & \\ & r & \end{array}$$

would show a proof of $p \Rightarrow r$ in which J justifies the conclusion q from p , while M explains why q and r are equivalent. In our proof we use \equiv and \Leftarrow , the latter connective being the converse of \Rightarrow , i.e., $(p \Rightarrow q) \equiv (q \Leftarrow p)$.

In writing quantified formulae, we use the angle brackets, $\langle \rangle$, to delineate the scope of the dummy, and the double colon, $::$, to separate the dummy from the quantified term, as in $\langle \forall x :: p.x \rangle$. Function application, as in the preceding “ $p.x$ ”, is denoted explicitly by an infix dot.

Besides “substituting equals for equals”, we use the Rule of Instantiation, viz., that for any expression y in the range of the dummy x

$$\langle \forall x :: p.x \rangle \Rightarrow p.y.$$

Twice we use it in its contrapositive form

$$\langle \exists x :: q.x \rangle \Leftarrow q.y.$$

In the context of the latter rule, expression y is often referred to as the *witness* for x . We write “ $x := y$ ” in a justification to denote that x is to be instantiated by y .

Type declarations consist of identifier and type (expression), separated by a colon. In what follows, x, Y, F, g are of the types

$$x : S, Y : \wp S, F : S \rightarrow \wp S, g : \wp S \rightarrow S,$$

while the constants $id : S \rightarrow S$ and $ID : \wp S \rightarrow \wp S$ denote the identity functions on S and $\wp S$ respectively. When x or Y are used as dummies, the range of the quantification is understood to extend over all elements of their type. Examples of well-typed boolean expressions are: $F.x = Y$, $g.Y = x$, $F.(g.Y) = Y$, $g.(F.x) = x$, $x \in Y$, $g.Y \in Y$, $x \in F.x$, $g.Y \in F.x$, etc.

2. THE DESIGN OF THE PROOF. We propose to prove the absence of a 1-1 correspondence between S and $\wp S$ by showing that for any F, g of the appropriate types

$$ID \neq F \circ g. \quad (0)$$

Remark We have already made a choice, since $id \neq g \circ F$ would have implied the absence of a 1-1 correspondence as well, but the trouble with the latter is that it is not a theorem, because F, g satisfying $F.x = \{x\}$ and $g.\{x\} = x$ provide a counterexample.

Our proof displays a sequence of boolean expressions, starting with (0) and ending with *true*, such that each expression implies its predecessor in the sequence. To construct the successor of (0) we propose to apply the definition of function (in)equality and record that (0) is equivalent to

$$\langle \exists Y :: ID.Y \neq (F \circ g).Y \rangle. \quad (1)$$

This wasn't the only choice possible, since $(p \neq q) \Leftarrow (h.p \neq h.q)$ for *any* function h , but the point is that, on our way from (0) to *true*, we must get rid of the constants ID and \circ , and we usually eliminate constants by appealing to their defining properties. Since both ID and \circ are defined in terms of function application, it stands to reason to apply both sides of (0) to some Y . Our remaining task is now to come up with a set-valued expression that can serve as a witness for Y .

We now eliminate ID and \circ by applying their definitions, i.e., we record that (1) is equivalent to

$$\langle \exists Y :: Y \neq F.(g.Y) \rangle, \quad (2)$$

and, doing justice to the fact that we are comparing subsets of S , we record that (2) is equivalent to

$$\langle \exists Y :: \langle \exists x :: x \in Y \neq x \in F.(g.Y) \rangle \rangle. \quad (3)$$

Remark The last two steps—elimination of ID , \circ and introduction of x —commute and could be done in the other order, but for the sake of brevity it is better to simplify first.

The inner existential quantification we have just introduced can be eliminated immediately by the instantiation $x := g.Y$ and we record that (3) is implied by

$$\langle \exists Y :: g.Y \in Y \neq g.Y \in F.(g.Y) \rangle. \quad (4)$$

This last implication depends on the monotonicity of existential quantification. This step was bold—it is our first strengthening in the sequence—and opportunistic: (i) we chose to instantiate x because at this stage we had no candidate witness for Y , and (ii) for better or for worse, we instantiated with $g.Y$ because we did not have much choice since $g.Y$ is the *only* element of S we can identify (and that is known to exist). Via the same instantiation, $x := g.Y$, we can now eliminate g and record that—again thanks to monotonicity of \exists —(4) is implied by

$$\langle \exists Y :: \langle \forall x :: x \in Y \equiv x \notin F.x \rangle \rangle, \quad (5)$$

where we have moved the negation to the right-hand side.

We could have performed the same transformation on (2), which would have yielded

$$\langle \exists Y :: \langle \forall x :: Y \neq F.x \rangle \rangle,$$

but this would not have helped in the construction of a witness for Y . With (5) we are in a much better position because thanks to set theory—which enables us to construct set-valued expressions—we can now rewrite (5) as the equivalent

$$\langle \exists Y :: Y = \{x \mid x \notin F.x\} \rangle. \quad (6)$$

Now the instantiation $Y := \{x \mid x \notin F.x\}$ stares us in the face and we accordingly record that (6) is implied by

$$\{x \mid x \notin F.x\} = \{x \mid x \notin F.x\}, \quad (7)$$

which, because of the reflexivity of $=$, is equivalent to

$$true. \quad (8)$$

3. A SUMMARY OF THE CALCULATION. We have included the heuristics in our argument for educational reasons. In a document written for another purpose one would omit them. By way of illustration we present the proof in Feijen's format, without the heuristics and incorporating somewhat larger steps:

$$\begin{aligned} & ID \neq F \circ g \\ \equiv & \{ \text{definition of } ID, \neq, \circ \} \\ & \langle \exists Y :: Y \neq F.(g.Y) \rangle \\ \Leftarrow & \{ (p \neq q) \Leftarrow (h.p \neq h.q) \} \\ & \langle \exists Y :: g.Y \in Y \neq g.Y \in F.(g.Y) \rangle \\ \Leftarrow & \{ \text{instantiation } x := g.Y \} \\ & \langle \exists Y :: \langle \forall x :: x \in Y \equiv x \notin F.x \rangle \rangle \\ \equiv & \{ \text{set theory: consider } \{x \mid x \notin F.x\} \text{ as witness for } Y \} \\ & true \end{aligned}$$

This presents the calculation in a degree of detail with which we expect most mathematicians to be perfectly happy most of the time. We did not mention in our hints the

monotonicity of \exists because we consider it part of the predicate calculus, which we feel free to use here without mention. We would like the reader to appreciate that we have combined (i) brevity, (ii) completeness—in the sense that the hints delineate where the justification is to be found—and (iii) the constructive path that leads to the “invention” $\{x \mid x \notin F.x\}$.

Comments There are several reasons for liking the calculational proof style. It provides heuristic guidance—as shown in our construction of the required set—and calculational proofs tend to be very compact and at the same time highly readable in the sense that they can be fully checked without pen and paper. More importantly, the design of calculational proofs is an art that seems eminently teachable.

ACKNOWLEDGMENT. Credit for the format in which we presented our calculational proof is due to W.H.J. Feijen. This format turned out to be an essential ingredient.

The University of Texas at Austin, Austin, TX 78712-1188
dijkstra@cs.utexas.edu
misra@cs.utexas.edu

For Every ε There Continuously Exists a δ

Giuseppe De Marco

A recent paper in this MONTHLY [1] proves the

Proposition. *Let X, Y be metric spaces, and let $f : X \rightarrow Y$ be a continuous map. There exists a continuous function $\delta : X \times]0, \infty[\rightarrow]0, \infty[$ such that if $|y - x| < \delta(x, \varepsilon)$ then $|f(y) - f(x)| < \varepsilon$, for every $x, y \in X$ and $\varepsilon > 0$ (we write $|x_1 - x_2|$ for the distance between x_1, x_2 , in any metric space considered).*

The proof given in [1] makes use of partitions of unity; still in [1] it is stated (added in proof) that this proposition is also obtained in [3] as a consequence of general results on multifunctions. Given the basic and pedagogical nature of the matter a really elementary and short proof of the Proposition is perhaps worth knowing; such a proof is reported both in [2] and in [3] and here is presented to the wider audience of the MONTHLY readership. It makes a nice exercise on product metric spaces.

Proof. To avoid trivialities, we assume that f is non-constant (for constant f , any strictly positive function δ will do). The map $(x, y, \varepsilon) \mapsto \varepsilon - |f(y) - f(x)|$ from $X \times X \times]0, \infty[$ into \mathbb{R} is clearly continuous if $X \times X \times]0, \infty[$ is given the product topology. It follows that the set

$$A = \{(x, y, \varepsilon) \in X \times X \times]0, \infty[: \varepsilon - |f(y) - f(x)| > 0\}$$

is open in $X \times X \times]0, \infty[$; its complement F is then closed, and it is non-empty since f is non-constant. The function $\text{dist}((x, y, \varepsilon), F)$ (distance from F) is then well-defined, Lipschitz continuous on $X \times X \times]0, \infty[$ (we take the box metric on this